

Commutative Algebra

Swayam Chube

Last Updated: January 28, 2026

I. A FIRST COURSE

§1 Valuation Rings

DEFINITION 1.1. An integral domain R with field of fractions K is said to be a *valuation ring* if for every $x \in K^\times$, $x \in R$ or $x^{-1} \in R$. We also say that R is a valuation ring of K .

PROPOSITION 1.2. Let R be a valuation ring of K . The R -submodules of K are totally ordered with respect to inclusion.

Proof. Let I and J be distinct R -submodules of K . If $I \setminus J \neq \emptyset$, pick $x \in I \setminus J$. For any $0 \neq y \in J$, one of xy^{-1} or $x^{-1}y$ must belong to R . If $xy^{-1} \in R$, then $x = y \cdot (xy^{-1}) \in J$, which is absurd. Thus $x^{-1}y \in R$, so that $y = x \cdot (x^{-1}y) \in I$, and hence, $J \subseteq I$. Argue similarly for the case $J \setminus I \neq \emptyset$. ■

COROLLARY 1.3. A valuation ring is local.

PROPOSITION 1.4. The following are equivalent for a ring R :

- (1) R is a valuation ring.
- (2) R is a local Bézout domain.

Proof. (1) \implies (2) follows immediately from Proposition 1.2, since any finitely generated ideal in R can be written as $a_1R + \cdots + a_nR$ for some $a_1, \dots, a_n \in R$.

(2) \implies (1): We must show that for every $x \in K^\times$, either $x \in R$ or $x^{-1} \in R$. Choose $f, g \in R$ such that $x = \frac{f}{g}$, and let $(h) = (f, g)$ as ideals in R . We can find $a, b \in R$ such that $f = ah$ and $g = bh$, and can find $c, d \in R$ such that $h = cf + dg$. Since R is a domain and $h \neq 0$, it follows that $ac + bd = 1$. Therefore, either a or b must be a unit in R , so that either $x \in R$ or $x^{-1} \in R$, thereby completing the proof. ■

PROPOSITION 1.5. A valuation ring is integrally closed.

Proof. Let (R, \mathfrak{m}) be a valuation ring with fraction field K . If $x \in K \setminus R$ is integral over R , then there is a non-trivial relation of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

with $a_i \in R$ for $0 \leq i \leq n-1$. Multiplying out by $x^{-n} \in \mathfrak{m}$, we have that $1 \in \mathfrak{m}$, a contradiction. Thus R is integrally closed. ■

REMARK 1.6. We note here that given a field K , a valuation ring of K is determined by its maximal ideal. Indeed, if (R, \mathfrak{m}) is a valuation ring of K , then we can write

$$K \setminus R = \{x^{-1} : x \in \mathfrak{m} \setminus \{0\}\}.$$

Further note that if R is a valuation ring of K , then any subring of K containing R is also a valuation ring of K .

THEOREM 1.7. Let R be a valuation ring of K and R' a subring of K containing R . Let \mathfrak{m} denote the maximal ideal of R , \mathfrak{p} the maximal ideal of R' , and suppose that $R \neq R'$. Then

- (1) $\mathfrak{p} \subsetneq \mathfrak{m} \subseteq R \subseteq R'$.
 - (2) \mathfrak{p} is a prime ideal of R and $R' = R_{\mathfrak{p}}$.
 - (3) R/\mathfrak{p} is a valuation ring of the field R'/\mathfrak{p} .
 - (4) Given a valuation ring \bar{S} of the field R/\mathfrak{m} , let S denote its preimage in R . Then S is a valuation ring of K and is called the *composite* of R and \bar{S} .
- Proof.*
- (1) Let $0 \neq x \in \mathfrak{p}$. Then $x^{-1} \in K \setminus R' \subseteq K \setminus R$, so that $x \in \mathfrak{m}$. Thus $\mathfrak{p} \subseteq \mathfrak{m}$. In light of Remark 1.6, $\mathfrak{p} \neq \mathfrak{m}$.
 - (2) Since $R/\mathfrak{p} \hookrightarrow R'/\mathfrak{p}$ as a subring, it is clear that \mathfrak{p} is a prime ideal in R . Further, since every element of $R \setminus \mathfrak{p}$ is invertible in R' , $R \subseteq R_{\mathfrak{p}} \subseteq R'$. Note that \mathfrak{p} is an ideal in $R_{\mathfrak{p}}$, and hence, $\mathfrak{p}R_{\mathfrak{p}} = \mathfrak{p}$, so that $R_{\mathfrak{p}} = R'$ due to (1).
 - (3) Straightforward.
 - (4) Let $\pi: R \rightarrow R/\mathfrak{m}$ denote the projection map. Note that $\mathfrak{m} \subseteq S$ and $S/\mathfrak{m} = \bar{S}$. If $x \in R \setminus S$, then $\pi(x) \notin \bar{S}$, and therefore, $\pi(x^{-1}) = \pi(x)^{-1} \in S$. Hence $x^{-1} \in S$. On the other hand, if $x \in K \setminus R$, then $x^{-1} \in \mathfrak{m} \subseteq S$. This shows that S is a valuation ring of K . ■

THEOREM 1.8. Let K be a field, $A \subseteq K$ a subring, and \mathfrak{p} a prime ideal of A . Then there exists a valuation ring (R, \mathfrak{m}) of K such that $A \subseteq R$, and $\mathfrak{m} \cap A = \mathfrak{p}$.

Proof. First, replacing A by $A_{\mathfrak{p}}$, we may assume that A is a local ring with maximal ideal \mathfrak{p} . Let \mathcal{F} denote the set of all subrings B of K containing A such that $1 \notin \mathfrak{p}B$. Clearly, every ascending chain in \mathcal{F} has an upper bound given by the union of all elements of the chain. Using Zorn's lemma, choose a maximal element R in \mathcal{F} . First, we contend that R is a local ring. Indeed, since $1 \notin \mathfrak{p}R$, there is a maximal ideal \mathfrak{m} of R containing $\mathfrak{p}R$. Note that $R_{\mathfrak{m}} \in \mathcal{F}$, so that $R = R_{\mathfrak{m}}$ in view of the maximality of R . Next, $\mathfrak{m} \cap A$ is a proper ideal containing \mathfrak{p} , which, due to the maximality of \mathfrak{p} must be equal to \mathfrak{p} .

It remains to show that R is a valuation ring of K . Suppose $x \in K$ is such that $x, x^{-1} \notin R$. Then $R \subsetneq R[x]$, and hence $1 \in \mathfrak{p}R[x]$, i.e., there is a polynomial relation

$$1 = a_0 + a_1x + \cdots + a_nx^n$$

with $a_i \in \mathfrak{p}R \subseteq \mathfrak{m}$ for $0 \leq i \leq n$. Multiplying by $(1 - a_0)^{-1} \in R$, one obtains a relation of the form

$$1 = b_1x + \cdots + b_nx^n$$

with $b_i \in \mathfrak{p}R$ for $1 \leq i \leq n$. Choose one such relation with the smallest possible value of n . Arguing similarly for x^{-1} , choose a relation

$$1 = c_1x^{-1} + \cdots + c_mx^{-m}$$

with the smallest possible value of m . If $n \geq m$, then multiply the second equation by $b_n x^n$ and subtract from the first to obtain a non-trivial relation of smaller degree than n , a contradiction. On the other hand, if $m > n$, then multiply the first relation by $c_m x^{-m}$ and subtract from the second to obtain a non-trivial relation of smaller degree than m , a contradiction again. Thus $x \in R$ or $x^{-1} \in R$, i.e., R is a valuation ring of K . ■

THEOREM 1.9. Let K be a field, $A \subseteq K$ a subring, and B the integral closure of A in K . Then B is equal to the intersection of all valuation rings of K containing A .

Proof. Let C denote the intersection of all valuation rings of K containing A . In view of Proposition 1.5, B is contained in every such valuation ring, so that $B \subseteq C$. Now let $x \in K$ be non-integral over A and set $y = x^{-1}$. Note that $1 \notin yA[y]$, else x would be integral over A . Let \mathfrak{p} be a maximal ideal of $A[y]$ containing $yA[y]$, and using Theorem 1.8, choose a valuation ring (R, \mathfrak{m}) of K containing $A[y]$ such that $\mathfrak{m} \cap A[y] = \mathfrak{p}$. In particular, $y \in \mathfrak{m}$, so that $x \notin R$. Thus $x \notin C$, as desired. ■

§§ Valuations

DEFINITION 1.10. An abelian group Γ together with a total order relation \leq is said to be *ordered* if for all $x, y \in \Gamma$ with $x \leq y$, $x + z \leq y + z$ for all $z \in \Gamma$.

Let K be a field. A *valuation* on K is a map $v: K \rightarrow \Gamma \cup \{\infty\}$ satisfying:

$$(i) \quad v(x) = \infty \text{ if and only if } x = 0,$$

$$(ii) \quad v(xy) = v(x) + v(y)^1, \text{ and}$$

$$(iii) \quad v(x+y) \geq \min\{v(x), v(y)\}$$

for all $x, y \in K$.

Corresponding to a valuation v on K , we can define

$$R_v = \{x \in K : v(x) \geq 0\} \quad \text{and} \quad \mathfrak{m}_v = \{x \in K : v(x) > 0\}.$$

It is not hard to see that (R_v, \mathfrak{m}_v) is a valuation ring of K . Conversely, we show that every valuation ring arises this way. Let

$$\Gamma = \{xR : x \in K^\times\}.$$

This is a group under the operation

$$(xR) \cdot (yR) = xyR$$

with neutral element R . Further, note that Γ is an ordered abelian group when equipped with the total ordering

$$xR \leq yR \iff xR \supseteq yR,$$

where we are implicitly invoking Proposition 1.2. Define $v: K \rightarrow \Gamma \cup \{\infty\}$ sending

$$v(x) = \begin{cases} xR & x \neq 0 \\ \infty & x = 0. \end{cases}$$

Note that $xR \geq R$ if and only if $xR \subseteq R$, that is, if $x \in R$. Hence, $R_v = R$ and $\mathfrak{m}_v = \mathfrak{m}$. This shows that every valuation ring arises from a valuation of K .

¹so that v is a group homomorphism when restricted to K^\times

DEFINITION 1.11. The *value group* of a valuation ring (R, \mathfrak{m}) of K is $v(K^\times)$, where v is a valuation of K such that $(R_v, \mathfrak{m}_v) = (R, \mathfrak{m})$.

To see that the value group is well-defined:

PROPOSITION 1.12. If v and v' are two valuations of K corresponding to the same valuation ring R and having value groups H and H' respectively, then there is an order-isomorphism $\varphi: H \rightarrow H'$ such that $v' = \varphi \circ v$.

Proof. Let $v: K^\times \rightarrow \Gamma$ and $v': K^\times \rightarrow \Gamma'$ be the two valuations. Define $\varphi: H \rightarrow H'$ by $\varphi(v(x)) = v'(x)$ for all $x \in K^\times$. We must show that φ is well-defined. Indeed, if $x, y \in K^\times$ are such that $v(x) = v(y)$, then $x^{-1}y$ is a unit in R , so that $v'(x^{-1}y) = 0$, i.e., $v'(x) = v'(y)$. That φ is a group homomorphism is clear. The surjectivity of φ is immediate from the fact that $v' = \varphi \circ v$. As for injectivity, if $\varphi(v(x)) = 0$, then $v'(x) = 0$, and hence x is a unit in R , so that $v(x) = 0$. Finally, if $v(x) \leq v(y)$, then $v(x^{-1}y) \geq 0$, so that $x^{-1}y \in R$, i.e., $v'(x^{-1}y) \geq 0$, that is, $v'(y) \geq v'(x)$. Thus φ is an order-isomorphism. ■

§2 Discrete Valuation Rings and Dedekind Domains

§§ Discrete Valuation Rings

DEFINITION 2.1. A valuation ring with value group order-isomorphic to \mathbb{Z} is called a *discrete valuation ring (DVR)*.

THEOREM 2.2. Let R be a valuation ring. Then the following are equivalent:

- (1) R is a DVR.
- (2) R is a PID.
- (3) R is Noetherian.

Proof. Let K be the field of fractions of R and \mathfrak{m} its maximal ideal.

(1) \Rightarrow (2) Let $v: K^\times \rightarrow \mathbb{Z}$ be a surjective valuation corresponding to R . Let $t \in \mathfrak{m}$ be such that $v(t) = 1$. For $0 \neq x \in \mathfrak{m}$, $v(x) = n > 0$ for some positive integer n . Then $v(x/t^n) = 0$, i.e., $x = ut^n$ for some unit $u \in R^\times$. In particular, this shows that $\mathfrak{m} = tR$. Now let $0 \neq I$ be a proper ideal in R , and let

$$n = \min \{v(a): 0 \neq a \in I\}.$$

Clearly n is a positive integer since I is proper. Let $x \in I$ with $v(x) = n$. Then $xR \subseteq I$, and for every $y \in I$, $v(y/x) \geq 0$, so that $y \in xR$. Thus $I = xR$, and R is a PID.

(2) \Rightarrow (3) is clear.

(3) \Rightarrow (2) A Noetherian Bézout domain is a PID.

(2) \Rightarrow (1) Let $t \in \mathfrak{m}$ be such that $\mathfrak{m} = tR$. Recall that a PID is a UFD, and let v denote the t -adic valuation on K . It is not hard to see that R is the valuation ring corresponding to v . ■

DEFINITION 2.3. If R is a DVR with maximal ideal \mathfrak{m} , then any element $t \in \mathfrak{m}$ such that $\mathfrak{m} = tR$ is said to be a *uniformizer* or a *uniformizing element* of R .

REMARK 2.4. We note here that a valuation ring whose maximal ideal is principal need not necessarily be a DVR. Indeed, let K be a field, (R, \mathfrak{m}_R) a DVR of K , set $k = R/\mathfrak{m}_R$, and suppose \mathfrak{N} is a DVR of k . Let S denote the composite of R and \mathfrak{N} . We contend that S is our desired counterexample.

Let $f \in \mathfrak{m}_R$ be a uniformizer of R , $g \in S$ such that $\bar{g} = g + \mathfrak{m}_R$ is a uniformizer of \mathfrak{N} . Then $\mathfrak{m}_S = \mathfrak{m}_R + gS$. Further, since $g \notin \mathfrak{m}_R$, it is a unit in R , so that $g^{-1} \in R$. Hence, for any element $h \in \mathfrak{m}_R$, we can write $h = g \cdot (g^{-1}h)$, so that $\mathfrak{m}_R \subseteq gS$. Hence $\mathfrak{m}_S = gS$ is principal.

Next, we show that S is not Noetherian. Indeed, consider the ascending chain of ideals in S :

$$(f) \subseteq (f, fg^{-1}) \subseteq (f, fg^{-1}, fg^{-2}) \subseteq \dots$$

We claim that all the above inclusions are proper. Indeed, if $fg^{-(n+1)} \in (f, fg^{-1}, \dots, fg^{-n})$ for some $n \geq 0$, then there exist $a_0, \dots, a_n \in S$ such that

$$fg^{-(n+1)} = a_0 f + a_1 fg^{-1} + \dots + a_n fg^{-n}.$$

Multiplying out by $f^{-1}g^{n+1}$, we obtain

$$a_0 g^{n+1} + \dots + a_n g = 1,$$

which is absurd, since $1 \notin \mathfrak{m}_S = gS$, thereby completing the proof.

THEOREM 2.5. Let R be a ring. The following conditions are equivalent:

- (1) R is a DVR.
- (2) R is a local PID but not a field.
- (3) R is a Noetherian local ring, $\dim R > 0$, and the maximal ideal of R is principal.
- (4) R is a one-dimensional normal Noetherian local domain.

Proof. (1) \Rightarrow (2) \Rightarrow (3) is clear.

(3) \Rightarrow (1) Let $\mathfrak{m} = tR$ denote the maximal ideal of R . Due to Krull's intersection theorem,

$$\bigcap_{n=1}^{\infty} \mathfrak{m}^n = (0).$$

Hence, for every $0 \neq x \in R$, there is a non-negative integer n such that $x \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$. Set $v(x) = n$. Now if $x, y \in R \setminus \{0\}$ are such that $v(x) = n$ and $v(y) = m$, then we can find units $u, v \in R^\times$ such that $x = t^n u$ and $y = t^m v$. This shows that $xy = t^{m+n} uv \neq 0$, so that R is an integral domain and $v(xy) = v(x) + v(y)$. Let K denote the fraction field of R , and set

$$v\left(\frac{a}{b}\right) = v(a) - v(b)$$

for all $a, b \in R \setminus \{0\}$. This is clearly well-defined, and defines a valuation on K whose value group is \mathbb{Z} and corresponding valuation ring is R . Hence R is a DVR.

(1) \Rightarrow (4) Recall that in a DVR the only ideals are (0) and powers of the maximal ideal. Thus the only prime ideals are (0) and \mathfrak{m} , so that $\dim R = 1$. That R is Noetherian follows from it being a PID, and finally recall that every valuation ring is normal.

(4) \Rightarrow (3) Let \mathfrak{m} denote the maximal ideal of R . Due to Nakayama's lemma and the fact that $\dim R = 1$, $\mathfrak{m} \neq \mathfrak{m}^2$. Choose $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. We shall show that $\mathfrak{m} = xR$. Note that $\mathfrak{m} \in \text{Ass}_R(R/xR)$, so that there exists $y \in R \setminus xR$ such that $(xR : y) = \mathfrak{m}$. Set $a = yx^{-1} \in K := \text{Frac}(R)$. Note that $a \notin R$ lest $y \in xR$. Set

$$\mathfrak{m}^{-1} := \{\alpha \in K : \alpha \mathfrak{m} \subseteq R\}.$$

Note that \mathfrak{m}^{-1} is an R -submodule of K , and further, by construction,

$$\mathfrak{m}\mathfrak{m}^{-1} := \{R\text{-submodule of } K \text{ generated by } x_i y_i : x_i \in \mathfrak{m}, y_i \in \mathfrak{m}^{-1}\} \subseteq R \quad \text{and} \quad R \subseteq \mathfrak{m}^{-1}.$$

In particular, we have the inclusions $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{m}^{-1} \subseteq R$. Hence, $\mathfrak{m}\mathfrak{m}^{-1} \in \{\mathfrak{m}, R\}$. If $\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{m}$, then $a\mathfrak{m} \subseteq \mathfrak{m}$. Since \mathfrak{m} is a finite R -module, due to Nakayama's lemma, a must be integral over R , but since R is normal, $a \in R$, a contradiction. Thus $\mathfrak{m}^{-1}\mathfrak{m} = R$. Next, note that $x\mathfrak{m}^{-1} \subseteq R$. If $x\mathfrak{m}^{-1} \subseteq \mathfrak{m}$, then

$$xR = x\mathfrak{m}^{-1}\mathfrak{m} \subseteq \mathfrak{m}^2,$$

a contradiction. Hence, $x\mathfrak{m}^{-1} = R$, so that

$$xR = x\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{m},$$

thereby completing the proof. ■

§§ Fractional Ideals and Dedekind domains

DEFINITION 2.6. Let R be an integral domain with fraction field K . An R -submodule I of K is said to be a *fractional ideal* if there is a non-zero $\alpha \in R$ such that $\alpha I \subseteq R$.

The standard operations on ideals readily generalize to operations on fractional ideals. Indeed, if I and J are fractional ideals, define

$$\begin{aligned} I + J &= \{x + y : x \in I, y \in J\} \\ IJ &= \{R\text{-submodule generated by } x_i y_i : x_i \in I, y_i \in J\}. \end{aligned}$$

Clearly, both $I + J$ and IJ are fractional ideals of R . Further, if $S \subseteq R$ is a multiplicative set, then

$$S^{-1}I = \left\{ \frac{x}{s} : x \in I, s \in S \right\}$$

is a fractional ideal of $S^{-1}R$.

LEMMA 2.7. Let R be an integral domain, M and N R -submodules of $K = \text{Frac}(R)$. If N is finitely generated, then

$$S^{-1}(M:N) = (S^{-1}M:S^{-1}N).$$

Proof. Clearly $S^{-1}(M:N) \subseteq (S^{-1}M:S^{-1}N)$. Since N is finitely generated, we can write $N = a_1R + \dots + a_nR$ for some $a_1, \dots, a_n \in K$. If $x \in (S^{-1}M:S^{-1}N)$, then for all $1 \leq i \leq n$, $xa_i \in S^{-1}M$. Therefore, there exist $c_i \in S$ such that $c_i xa_i \in M$, whence $c_i x \in (M:N)$, so that $x \in S^{-1}(M:N)$. ■

DEFINITION 2.8. An R -submodule I of K is said to be *invertible* if there exists an R -submodule J of K such that $IJ = R$.

PROPOSITION 2.9. An invertible R -submodule of K must be a finite R -module.

Proof. Let I be an invertible fractional ideal of R and J an R -submodule of K such that $IJ = R$. Then we can find $a_1, \dots, a_n \in I$ and $b_1, \dots, b_n \in J$ such that

$$1 = a_1 b_1 + \dots + a_n b_n.$$

For each $x \in I$, we can write

$$x = (xb_1)a_1 + \dots + (xb_n)a_n,$$

and note that $xb_i \in R$ for $1 \leq i \leq n$. It follows that $I = a_1R + \dots + a_nR$. ■

COROLLARY 2.10. Every invertible R -submodule of K is a fractional ideal.

REMARK 2.11. Suppose I is an invertible fractional ideal of R , and set

$$I^{-1} := \{\alpha \in K : \alpha I \subseteq R\}.$$

This is clearly an R -submodule of K . Further, note that $II^{-1} \subseteq R$, so that

$$I^{-1} = JII^{-1} \subseteq J.$$

But since $JI \subseteq R$, we clearly have $J \subseteq I^{-1}$. This shows that $J = I^{-1}$.

THEOREM 2.12. Let R be an integral domain and I an R -submodule of K . The following are equivalent:

- (1) I is an invertible fractional ideal.
- (2) I is a projective R -module.
- (3) I is a finite R -module, and for each maximal ideal \mathfrak{m} of R , the fractional ideal $I_{\mathfrak{m}} := IR_{\mathfrak{m}}$ of $R_{\mathfrak{m}}$ is principal.

Proof. (1) \Rightarrow (2) Let $a_1, \dots, a_n \in I$ and $b_1, \dots, b_n \in I^{-1}$ be such that $1 = a_1b_1 + \dots + a_nb_n$. As we have seen in the proof of Proposition 2.9, $I = a_1R + \dots + a_nR$. Let $\pi: F := \bigoplus_{i=1}^n Re_i \rightarrow I$ be the map sending $e_i \mapsto a_i$. Define $\sigma: I \rightarrow F$ by

$$\sigma(x) = (xb_1)e_1 + \dots + (xb_n)e_n.$$

It is then clear that $\pi \circ \sigma = \text{id}_I$, so that I is projective.

(2) \Rightarrow (1) There is a free module $F = \bigoplus_i Re_i$ and an epimorphism $\pi: F \rightarrow I$ which splits through an R -linear map $\sigma: I \rightarrow F$. Let $a_i = \pi(e_i)$ and $\lambda_i = \pi_i \circ \sigma: I \rightarrow R$. Note that every R -linear map $I \rightarrow R$ is multiplication by some element of K . Say $\lambda_i(x) = b_i x$ for all $x \in I$. Note that $b_i \in I^{-1}$ for all i . Then

$$\pi(\sigma(x)) = \sum_i a_i b_i x \implies \sum_i a_i b_i = 1.$$

Set J denote the R -submodule of K generated by the b_i 's. Then $R \subseteq IJ \subseteq R$, and hence I is an invertible fractional ideal.

(1) \Rightarrow (3) That I is a finite R -module is the content of Proposition 2.9. Further,

$$R_{\mathfrak{m}} = (II^{-1})_{\mathfrak{m}} = I_{\mathfrak{m}}(I^{-1})_{\mathfrak{m}},$$

so that $I_{\mathfrak{m}}$ is an invertible fractional ideal of $R_{\mathfrak{m}}$. Due to (2), $I_{\mathfrak{m}}$ is a projective $R_{\mathfrak{m}}$ -module. But since any two elements of K are $R_{\mathfrak{m}}$ -linearly dependent, $I_{\mathfrak{m}}$ must be principal.

(3) \Rightarrow (1) Note that for every maximal ideal \mathfrak{m} of R ,

$$(I^{-1})_{\mathfrak{m}} = (R : I)_{\mathfrak{m}} = (R_{\mathfrak{m}} : I_{\mathfrak{m}}) = (I_{\mathfrak{m}})^{-1}.$$

If $II^{-1} \subsetneq R$, then there is a maximal ideal \mathfrak{m} containing II^{-1} , so that

$$\mathfrak{m}R_{\mathfrak{m}} \supseteq (II^{-1})_{\mathfrak{m}} = I_{\mathfrak{m}}(I^{-1})_{\mathfrak{m}} = I_{\mathfrak{m}}I_{\mathfrak{m}}^{-1} = R_{\mathfrak{m}},$$

a contradiction. This completes the proof. ■

THEOREM 2.13. Let R be a Noetherian domain, and \mathfrak{p} a non-zero prime ideal of R . If \mathfrak{p} is invertible, then $\text{ht}\mathfrak{p} = 1$ and $R_{\mathfrak{p}}$ is a DVR.

Proof. Since \mathfrak{p} is invertible, due to Theorem 2.12, $\mathfrak{p}R_{\mathfrak{p}}$ is a principal ideal. Since $\dim R_{\mathfrak{p}} = \text{ht}\mathfrak{p} > 0$, it follows from Theorem 2.5 that $R_{\mathfrak{p}}$ is a DVR, and hence $\text{ht}\mathfrak{p} = \dim R_{\mathfrak{p}} = 1$. ■

THEOREM 2.14. Let R be a normal Noetherian domain. Then

- (1) all prime divisors of a non-zero principal ideal have height 1.

$$(2) R = \bigcap_{\text{ht}\mathfrak{p}=1} R_{\mathfrak{p}}.$$

Proof. (1) This follows from Krull's Hauptidealsatz.

- (2) Suppose $\frac{a}{b} \in \bigcap_{\text{ht}\mathfrak{p}=1} R_{\mathfrak{p}}$ with $b \neq 0$. We shall show that $a \in bR$. If b is a unit in R , then there is nothing to prove. If b is not a unit in R , consider the primary decomposition

$$bR = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$$

with corresponding associated primes $\mathfrak{p}_1, \dots, \mathfrak{p}_r$. Due to (1), we know that $\text{ht}\mathfrak{p}_i = 1$ for all i , so that there are no embedded associated primes. Localising at \mathfrak{p}_i and contracting back to R , we have

$$\mathfrak{q}_i = bR_{\mathfrak{p}} \cap R \ni a.$$

Therefore,

$$a \in \bigcap_{i=1}^r \mathfrak{q}_i = bR,$$

as desired. ■

PORISM 2.15. Let R be a Noetherian domain. If all associated primes of a non-zero principal ideal have height 1, then

$$R = \bigcap_{\text{ht}\mathfrak{p}=1} R_{\mathfrak{p}}.$$

COROLLARY 2.16. Let R be a Noetherian domain. Then R is normal if and only if the following two conditions are satisfied:

- (i) for every height 1 prime \mathfrak{p} , $R_{\mathfrak{p}}$ is a DVR; and
- (ii) all associated primes of a non-zero principal ideal of R have height 1.

Proof. Necessity is the content of Theorem 2.14. For sufficiency, note that due to Porism 2.15, $R = \bigcap_{\text{ht}\mathfrak{p}=1} R_{\mathfrak{p}}$. But since each $R_{\mathfrak{p}}$ is a DVR, it is normal, so that R is normal. ■

DEFINITION 2.17. An integral domain for which every ideal is invertible is called a *Dedekind domain*.

THEOREM 2.18. For an integral domain R , the following conditions are equivalent:

- (1) R is a Dedekind domain.
- (2) R is either a field or a one-dimensional Noetherian normal domain.
- (3) every non-zero ideal of R can be written as a product of a finite number of prime ideals.

Proof. (1) \implies (2) Suppose R is a field. Since every ideal is invertible, it is finitely generated, so that R is Noetherian. If \mathfrak{p} is a non-zero prime ideal of R , then due to Theorem 2.12, $\mathfrak{p}R_{\mathfrak{p}}$ is a principal ideal. Due to Theorem 2.5, $R_{\mathfrak{p}}$ is a DVR and $\text{ht } \mathfrak{p} = 1$. Since R is not a field, every prime ideal is a maximal ideal, and hence, we can write

$$R = \bigcap_{0 \neq \mathfrak{p} \in \text{Spec } R} R_{\mathfrak{p}}.$$

Being the intersection of normal domains, R is also a normal domain.

(2) \implies (1) Let I be an ideal of R . We shall show that I is invertible. For a maximal ideal \mathfrak{m} of R , note that $R_{\mathfrak{m}}$ is a one-dimensional Noetherian normal local ring, which, due to Theorem 2.5, is a DVR. In particular, $IR_{\mathfrak{m}}$ is a principal ideal. Thus, due to Theorem 2.12, I is invertible.

(1) \implies (3) That R is Noetherian follows from (2). We prove (3) by Noetherian induction. Let \mathcal{F} denote the set of all non-zero proper ideals in R that are not products of prime ideals. If \mathcal{F} is non-empty, using the Noetherian-ness of R , choose a maximal element $I \in \mathcal{F}$. Note that every proper ideal of R properly containing I can be expressed as a product of prime ideals. Let \mathfrak{m} be a maximal ideal containing I . Clearly $I \neq \mathfrak{m}$ else it has a trivial expression as a product of prime ideals. Since $R \subseteq \mathfrak{m}^{-1}$, we have $I \subseteq I\mathfrak{m}^{-1} \subseteq \mathfrak{m}\mathfrak{m}^{-1} = R$. If $I\mathfrak{m}^{-1} = I$, then due to Nakayama's lemma, every element of \mathfrak{m}^{-1} would be integral over R , and therefore must be an element of R due to (2), a contradiction. Thus $I\mathfrak{m}^{-1} \supsetneq I$, so that it can be expressed as a product of prime ideals. Multiplying this expression by \mathfrak{p} , we see that I can be expressed as a product of prime ideals too, a contradiction. Thus \mathcal{F} is empty, as desired.

(3) \implies (1) We shall show that every prime ideal in R is invertible. The factorization property would then imply the same for all non-zero ideals of R .

Step 1. Suppose I and J are fractional ideals of R such that $B = IJ$ is an invertible fractional ideal. We shall show that I and J are invertible. First, note that

$$I^{-1}J^{-1}B = I^{-1}J^{-1}JI \subseteq R \implies I^{-1}J^{-1} = I^{-1}J^{-1}BB^{-1} \subseteq B^{-1}.$$

Also, since $B^{-1}IJ = R$, we have the two obvious inclusions $B^{-1}I \subseteq J^{-1}$ and $B^{-1}J \subseteq I^{-1}$. Multiplying these two inclusions, we obtain

$$B^{-1} \subseteq I^{-1}J^{-1} \implies I^{-1}J^{-1} = B^{-1}.$$

Finally, note that

$$R = BB^{-1} = (II^{-1})(JJ^{-1}),$$

so that $II^{-1} = JJ^{-1} = R$, i.e., I and J are invertible.

Step 2. Let \mathfrak{p} be a non-zero prime ideal in R . We shall show that for any ideal I of R properly containing \mathfrak{p} , $\mathfrak{p} = I\mathfrak{p}$. To this end, it suffices to show that $\mathfrak{p} \subseteq I\mathfrak{p}$. Let $a \in I \setminus \mathfrak{p}$ and set $J = aR + \mathfrak{p}$. It suffices to show that $\mathfrak{p} \subseteq J\mathfrak{p}$ so that we may replace I by J and continue our analysis. Consider prime decompositions of the two ideals

$$I^2 = \mathfrak{p}_1 \cdots \mathfrak{p}_r \quad \text{and} \quad a^2R + \mathfrak{p} = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Clearly each of the \mathfrak{q}_i 's contain \mathfrak{p} . Since $I^2 \subseteq \mathfrak{p}_i$, we have $I \subseteq \mathfrak{p}_i$, so that $\mathfrak{p} \subseteq \mathfrak{p}_i$. Let $\bar{R} := R/\mathfrak{p}$, and for each $x \in R$, let \bar{x} denote its image in \bar{R} . Note that \bar{R} is an integral domain with the factorization property (3), and in \bar{R} , we have the decompositions

$$\bar{\mathfrak{p}}_1 \cdots \bar{\mathfrak{p}}_r = \bar{a}^2 \bar{R} = \bar{\mathfrak{q}}_1 \cdots \bar{\mathfrak{q}}_s.$$

Since $\bar{a}^2 \bar{R}$ is an invertible ideal of \bar{R} , due to Step 1, all the $\bar{\mathfrak{p}}_i$'s and the $\bar{\mathfrak{q}}_j$'s are invertible ideals of \bar{R} . Now let $\bar{\mathfrak{p}}_1$ be a minimal element of the set $\{\bar{\mathfrak{p}}_1, \dots, \bar{\mathfrak{p}}_r\}$. Since $\bar{\mathfrak{p}}_1 \supseteq \bar{\mathfrak{q}}_1 \cdots \bar{\mathfrak{q}}_s$, using Prime Avoidance, $\bar{\mathfrak{p}}_1$

must contain one of the \bar{q}_i 's, say without loss of generality, \bar{q}_1 . An analogous argument would give that \bar{q}_1 must contain some \bar{p}_j , which, due to the minimality of \bar{p}_1 must be equal to \bar{p}_1 – that is, $\bar{p}_1 = \bar{q}_1$. Since these ideals are invertible, multiplying with their inverses, we are left with

$$\bar{p}_2 \cdots \bar{p}_r = \bar{q}_2 \cdots \bar{q}_s.$$

Continuing in this way, we obtain $r = s$ and $\bar{p}_i = \bar{q}_i$ for $1 \leq i \leq r$. In particular, $p_i = q_i$ for $1 \leq i \leq r$, so that

$$a^2R + p = (aR + p)^2 = a^2R + ap + p^2.$$

Hence, every $x \in p$ can be written as

$$x = a^2y + az + w \quad \text{where } y \in R, z \in p, \text{ and } w \in p^2.$$

Thus $a^2y \in p$ – but since $a \notin p$, $y \in p$. This gives

$$p \subseteq ap + p^2 = I_p,$$

as desired.

Step 3. Let $0 \neq a \in R$. Then in the factorization $bR = p_1 \cdots p_r$, all the p_i 's are maximal. Indeed, if I is any ideal properly containing p_i , then due to Step 2, $p_i = I_{p_i}$. As we have already argued, every p_i is invertible, so that $I = R$.

Step 4. Let p be a non-zero prime ideal in R , and let $0 \neq a \in R$. If $aR = p_1 \cdots p_r$, then due to Step 3, each p_i is maximal. Since $p \supseteq aR$, there is an index i such that $p_i \subseteq p$. The maximality of p_i forces $p_i = p$. In particular, p is invertible, thereby completing the proof. ■

§3 Dimension Theory

§§ Hilbert Polynomials

THEOREM 3.1. An \mathbb{N} -graded ring $R = \bigoplus_{n \geq 0} R_n$ is Noetherian if and only if R_0 is Noetherian and R is a finitely generated R_0 -algebra.

Proof. The converse direction follows from Hilbert's basis theorem. We prove the forward direction. Suppose R is a Noetherian ring. Since $R_0 = R/R_+$ where $R_+ = \bigoplus_{n > 0} R_n$, it follows that R_0 is Noetherian.

Next, since R_+ is a finitely generated ideal, we may pick homogeneous elements $x_1, \dots, x_r \in R_+$ generating it as an R -module. Using induction on $n \geq 0$, we shall show that $R_n \subseteq R_0[x_1, \dots, x_r]$ for all $n \geq 0$. Let $d_i > 0$ denote the degree of x_i . Then

$$R_n = \sum_{i=1}^r x_i R_{n-d_i},$$

with the convention that $R_j = 0$ for $j < 0$. Using the inductive hypothesis, every element of R_{n-d_i} can be written as a polynomial in the x_i 's with coefficients in R_0 . From the above relation, it follows that every element of R_n can be written as a polynomial in the x_i 's with coefficients in R_0 . ■

PROPOSITION 3.2. Let $R = \bigoplus_{n \geq 0} R_n$ be a Noetherian graded ring, and $M = \bigoplus_{n \geq 0} M_n$ a finite graded R -module. Then each M_n is a finite R_0 -module.

Proof. The case $M = R$ has been dealt with in the proof of Theorem 3.1. We may choose the generators $\omega_1, \dots, \omega_r$ of M as an R -module to be homogeneous. Let d_i denote the degree of each ω_i . Note that $M_+ := \bigoplus_{n \geq 0} M_n$ is a submodule of M , it follows that $M_0 = M/M_+$ is a finite R -module which is annihilated by R_+ . Therefore, M_0 is a finite R -module. Next, for $n > 0$, we can write

$$M_n = \sum_{i=1}^r R_{n-d_i} \omega_i.$$

Since each R_j is a finite R_0 -module, it follows that each M_n is a finite R_0 -module. ■

DEFINITION 3.3. Let $R = \bigoplus_{n \geq 0} R_n$ be a Noetherian graded ring with R_0 Artinian. For a finite graded R -module $M = \bigoplus_{n \geq 0} M_n$, we define its *Hilbert series* to be

$$P(M, t) := \sum_{n=0}^{\infty} \lambda_{R_0}(M_n) t^n \in \mathbb{Z}[[t]].$$

Note that each M_n is a finite R_0 -module, and hence, is Artinian, so that it has finite length as an R_0 -module.

THEOREM 3.4 (HILBERT-SERRE). Let $R = \bigoplus_{n \geq 0} R_n$ be a Noetherian graded ring with R_0 Artinian, and let $M = \bigoplus_{n \geq 0} M_n$ be a finite graded R -module. Suppose $x_1, \dots, x_r \in R$ are homogeneous elements such that R is generated by x_1, \dots, x_r as an R_0 -algebra. If each x_i has degree $d_i > 0$, then the Hilbert series $P(M, t)$ is a rational function, that is, there is a polynomial $f(t) \in \mathbb{Z}[t]$ such that

$$P(M, t) = \frac{f(t)}{\prod_{i=1}^r (1 - t^{d_i})} \quad \text{in } \mathbb{Z}[[t]].$$

Proof. We shall prove this statement by induction on $r \geq 0$. If $r = 0$, then $R = R_0$, so that M is an Artinian R -module. Since there is a descending chain of R -submodules

$$M \supseteq \bigoplus_{n \geq 1} M_n \supseteq \bigoplus_{n \geq 2} M_n \supseteq \cdots,$$

we must have that $M_n = 0$ for $n \gg 0$, that is, $P(M, t)$ is a polynomial in t , thereby establishing the theorem in this case.

Suppose now that $r > 0$. For $n \geq 0$, let K_n and L_{n+d_r} denote the kernel and cokernel of the map $M_n \xrightarrow{x_r} M_{n+d_r}$. The short exact sequence

$$0 \rightarrow K_n \rightarrow M_n \xrightarrow{x_r} M_{n+d_r} \rightarrow L_{n+d_r} \rightarrow 0$$

gives us

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+d_r}) - \lambda(L_{n+d_r}) = 0. \tag{1}$$

The above convention is such that $L_n = M_n$ for $n < d_r$. Set $K = \bigoplus_{n \geq 0} K_n$ and $L = \bigoplus_{n \geq 0} L_n$. Note that K_n is annihilated by x_r , and since $L = M/x_r M$ as a graded R -module, it is also annihilated by x_r . In particular, K and L are graded $\bar{R} := R/x_r R$ -modules. Multiplying the above equation by t^{n+d_r} and summing over $n \in \mathbb{Z}$, we obtain:

$$t^{d_r} P(K, t) - t^{d_r} P(M, t) + P(M, t) - P(L, t) = 0.$$

Since \overline{R} is an R_0 -algebra generated by x_1, \dots, x_{r-1} , the induction hypothesis applies so that there are polynomials $g(t), h(t) \in \mathbb{Z}[t]$ such that

$$P(K, t) = \frac{g(t)}{\prod_{i=1}^{r-1} (1 - t^{d_i})} \quad \text{and} \quad P(L, t) = \frac{h(t)}{\prod_{i=1}^{r-1} (1 - t^{d_i})},$$

whence the conclusion follows. \blacksquare

DEFINITION 3.5. In Theorem 3.4 if $d_1 = \dots = d_r = 1$, then there is an integer polynomial $f(t) \in \mathbb{Z}[t]$ with $f(1) \neq 0$ and a $d \geq 0$ such that

$$P(M, t) = \frac{f(t)}{(1-t)^d} \in \mathbb{Z}[[t]].$$

This integer d is denoted by $d(M)$.

COROLLARY 3.6. If $d_1 = \dots = d_r = 1$ in Theorem 3.4 and $d = d(M)$, then there is a polynomial $\varphi_M(X) \in \mathbb{Q}[X]$ such that for $n \gg 0$, $\lambda(M_n) = \varphi_M(n)$.

DEFINITION 3.7. The polynomial $\varphi_M(X) \in \mathbb{Q}[X]$ is called the *Hilbert polynomial* of the graded R -module M .

§§ Samuel Functions

Let (A, \mathfrak{m}) be a Noetherian local ring, M a finite A -module, and \mathfrak{q} an \mathfrak{m} -primary ideal. The maximal ideal defines filtrations on A and M :

$$A \supseteq \mathfrak{q} \supseteq \mathfrak{q}^2 \supseteq \dots \quad \text{and} \quad M \supseteq \mathfrak{q}M \supseteq \mathfrak{q}^2M \supseteq \dots$$

Let

$$\text{gr}_{\mathfrak{q}}(A) := \bigoplus_{n \geq 0} \mathfrak{q}^n / \mathfrak{q}^{n+1} \quad \text{and} \quad \text{gr}_{\mathfrak{q}}(M) := \bigoplus_{n \geq 0} \frac{\mathfrak{q}^n M}{\mathfrak{q}^{n+1} M}$$

denote the corresponding associated graded objects. Note that $\text{gr}_{\mathfrak{q}}(M)$ is a finite graded $\text{gr}_{\mathfrak{q}}(A)$ -module. If \mathfrak{q} is generated as an A -module by x_1, \dots, x_r , and $\bar{x}_1, \dots, \bar{x}_r \in \mathfrak{q}/\mathfrak{q}^2$ denote the corresponding images, then $\text{gr}_{\mathfrak{q}}(A)$ is generated as an A/\mathfrak{q} -algebra by $\bar{x}_1, \dots, \bar{x}_r$, which are homogeneous elements of degree 1. Further, since A/\mathfrak{q} is Artinian, we may talk about the Hilbert series of $\text{gr}_{\mathfrak{q}}(M)$ with respect to $\text{gr}_{\mathfrak{q}}(A)$. Now define

$$\chi_M^{\mathfrak{q}}(n) = \sum_{i=0}^n \lambda_{A/\mathfrak{q}} \left(\frac{\mathfrak{q}^i M}{\mathfrak{q}^{i+1} M} \right) = \lambda_{A/\mathfrak{q}} \left(\frac{M}{\mathfrak{q}^{n+1} M} \right).$$

Recall from Corollary 3.6 that $\lambda_{A/\mathfrak{q}} \left(\frac{\mathfrak{q}^n M}{\mathfrak{q}^{n+1} M} \right)$ is a polynomial of degree $d(\text{gr}_{\mathfrak{q}}(M))$ for $n \gg 0$. It follows that $\chi_M^{\mathfrak{q}}(n)$ is a polynomial of degree $d(\text{gr}_{\mathfrak{q}}(M)) + 1$ for $n \gg 0$.

PROPOSITION 3.8. If \mathfrak{p} and \mathfrak{q} are two \mathfrak{m} -primary ideals, then $\deg \chi_M^{\mathfrak{p}} = \deg \chi_M^{\mathfrak{q}}$.

Proof. There are integers $a > 0$ and $b > 0$ such that $\mathfrak{p}^a \subseteq \mathfrak{q}$ and $\mathfrak{q}^b \subseteq \mathfrak{p}$. Thus, $\mathfrak{p}^{a(n+1)} \subseteq \mathfrak{q}^{n+1}$ and $\mathfrak{q}^{b(n+1)} \subseteq \mathfrak{p}^{n+1}$. In particular, this gives the inequalities

$$\chi_M^{\mathfrak{p}}(a(n+1)-1) \geq \chi_M^{\mathfrak{q}}(n) \quad \text{and} \quad \chi_M^{\mathfrak{q}}(b(n+1)-1) \geq \chi_M^{\mathfrak{p}}(n)$$

for every positive integer n . Thus $\deg \chi_M^{\mathfrak{p}} = \deg \chi_M^{\mathfrak{q}}$, as desired. \blacksquare

DEFINITION 3.9. We write $d(M)$ to denote $\deg \chi_M^{\mathfrak{q}}$ for some \mathfrak{m} -primary ideal \mathfrak{q} .

THEOREM 3.10. Let (A, \mathfrak{m}) be a Noetherian local ring and $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ a short exact sequence of finite A -modules. Then

$$d(M) = \max \{d(M'), d(M'')\}.$$

Further, if \mathfrak{q} is an \mathfrak{m} -primary ideal of A , then $\chi_M^{\mathfrak{q}} - \chi_{M''}^{\mathfrak{q}}$ and $\chi_{M'}^{\mathfrak{q}}$ have the same leading coefficient.

Proof. Let \mathfrak{q} be an \mathfrak{m} -primary ideal and let $\lambda := \lambda_{A/\mathfrak{q}}$ for brevity. Further, we may assume that $M' \subseteq M$ and $M'' = M/M'$. We have

$$\chi_{M''}^{\mathfrak{q}}(n) = \lambda \left(\frac{M''}{\mathfrak{q}^{n+1} M''} \right) = \lambda \left(\frac{M}{M' + \mathfrak{q}^{n+1} M} \right) = \lambda \left(\frac{M}{\mathfrak{q}^{n+1} M} \right) - \underbrace{\lambda \left(\frac{M' + \mathfrak{q}^{n+1} M}{\mathfrak{q}^{n+1} M} \right)}_{\varphi(n)}.$$

Note that $\varphi(n)$ is a polynomial for $n \gg 0$. Note that

$$\frac{M' + \mathfrak{q}^{n+1} M}{\mathfrak{q}^{n+1} M} = \frac{M'}{M' \cap \mathfrak{q}^{n+1} M},$$

and from the Artin-Rees lemma, we know that the filtration $(M' \cap \mathfrak{q}^{n+1})_{n \geq 0}$ is \mathfrak{q} -stable. In particular, there is an integer $N > 0$ such that whenever $n > N$, we have

$$\mathfrak{q}^{n+1} M' \subseteq M' \cap \mathfrak{q}^{n+1} M = \mathfrak{q}^{n-N} (M' \cap \mathfrak{q}^{N+1} M) \subseteq \mathfrak{q}^{n-N} M'.$$

This gives $\chi_{M'}^{\mathfrak{q}}(n) \geq \varphi(n) \geq \chi_{M'}^{\mathfrak{q}}(n-N)$ for all $n > N$. This shows that $\deg \varphi = d(M')$ and φ and $\chi_{M'}^{\mathfrak{q}}$ have the same leading coefficient. The conclusion now follows, since all polynomials involved have positive leading coefficients. ■

COROLLARY 3.11. If $M \twoheadrightarrow N$ is an epimorphism of A -modules, then $d(N) \leq d(M)$.

Proof. Apply the theorem to the short exact sequence $0 \rightarrow \ker \rightarrow M \rightarrow N \rightarrow 0$. ■

DEFINITION 3.12. Let (A, \mathfrak{m}) be a Noetherian local ring and M a finite A -module. We define the *Chevalley dimension* of M to be

$$\delta(M) := \inf \left\{ n : \exists x_1, \dots, x_n \in \mathfrak{m} \text{ such that } \lambda_A \left(\frac{M}{(x_1, \dots, x_n)M} \right) < \infty \right\}.$$

THEOREM 3.13 (DIMENSION THEOREM). Let (A, \mathfrak{m}) be a Noetherian local ring and M a finite A -module. Then

$$\dim \text{Supp}_R(M) =: \dim M = d(M) = \delta(M).$$

Proof. We prove this theorem in three steps by proving the sequence of inequalities $\dim M \leq d(M) \leq \delta(M) \leq \dim M$.

Step 1. We show that $d(M) \geq \dim M$. To this end, we first establish this inequality for $M = A$ by induction on $d(A)$. If $d(A) = 0$, then $\lambda(A/\mathfrak{m}^n)$ is eventually constant, so that $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for $n \gg 0$, equivalently, due to Nakayama's lemma, $\mathfrak{m}^n = 0$, that is, $\dim A = 0$. Next, suppose $d(A) > 0$ and consider a strictly ascending chain of prime ideals $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \dots \subseteq \mathfrak{p}_e$. If $e = 0$, then there is nothing to prove. Suppose now that $e > 0$ and choose $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$. Let $B = A/(\mathfrak{p}_0 + xA)$, which is a ring and an A -module fitting into a short exact sequence of A -modules

$$0 \rightarrow A/\mathfrak{p}_0 \xrightarrow{x} A/\mathfrak{p}_0 \rightarrow B \rightarrow 0.$$

Due to Theorem 3.10, $d_A(B) < d_A(A/\mathfrak{p}_0) \leq d_A(A)$. Further, using the induction hypothesis, $\dim B \leq d_B(B) = d_A(B) < d_A(A)$. Since the image of the strictly ascending chain of prime ideals $\mathfrak{p}_1 \subseteq \dots \subseteq \mathfrak{p}_e$ in B is also a strictly ascending chain of prime ideals, $e - 1 < d_A(A)$, so that $e \leq d_A(A)$. Taking a supremum over all such e 's, $\dim A \leq d(A)$.

Now, let M be a finite A -module. One can find a filtration

$$0 = M_0 \subseteq M_1 \subseteq \dots \subseteq M_r = M$$

such that $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ as an A -module for some prime ideal \mathfrak{p}_i . Repeatedly invoking Theorem 3.10,

$$d(M) = \sup_{1 \leq i \leq r} d_A(A/\mathfrak{p}_i) = \sup_{1 \leq i \leq r} d_{A/\mathfrak{p}_i}(A/\mathfrak{p}_i) \geq \sup_{1 \leq i \leq r} \dim A/\mathfrak{p}_i = \dim M,$$

since $\text{Supp}_R(M) = V(\mathfrak{p}_1) \cup \dots \cup V(\mathfrak{p}_r)$, as desired.

Step 2. We show that $\delta(M) \geq d(M)$. Let $s = \delta(M)$. If $s = 0$, then M is Artinian, so that $\lambda_R(M) < \infty$, i.e., $\underline{\chi_M^m}$ is bounded, and hence $d(M) = 0$.

Let $x_1, \dots, x_s \in \mathfrak{m}$ be such that $\lambda_A\left(\frac{M}{(x_1, \dots, x_s)M}\right) < \infty$, and set $M_i = M/(x_1, \dots, x_i)M$. Clearly $\delta(M_i) = s - i$. Further, we have

$$\begin{aligned} \lambda_R(M_1/\mathfrak{m}^n M_1) &= \lambda_R\left(\frac{M}{x_1 M + \mathfrak{m}^n M}\right) \\ &= \lambda_R(M/\mathfrak{m}^n M) - \lambda_R\left(\frac{x_1 M + \mathfrak{m}^n M}{\mathfrak{m}^n M}\right). \end{aligned}$$

The map $M \xrightarrow{x_1} M/\mathfrak{m}^n M$ has kernel $(\mathfrak{m}^n M : x_1)$ and image equal to $\frac{x_1 M + \mathfrak{m}^n M}{\mathfrak{m}^n M}$, and hence

$$\lambda_R(M_1/\mathfrak{m}^n M_1) = \lambda_R(M/\mathfrak{m}^n M) - \lambda_R\left(\frac{M}{(\mathfrak{m}^n : x_1)M}\right) \geq \lambda_R(M/\mathfrak{m}^n M) - \lambda_R(M/\mathfrak{m}^{n-1}M) = \lambda_R(\mathfrak{m}^{n-1}M/\mathfrak{m}^n M).$$

The right hand side is a polynomial of degree $d(M) - 1$ for $n \gg 0$. Thus $d(M_1) \geq d(M) - 1$. Inductively, $d(M_i) \geq d(M) - i$, in particular, $0 = d(M_s) \geq d(M) - s$, whence $\delta(M) \geq d(M)$.

Step 3. Finally, we show that $\dim M \geq \delta(M)$ by induction on $\dim M$. If $\dim M = 0$, then $\text{Supp}_R(M) = \{\mathfrak{m}\}$, so that $\lambda_R(M) < \infty$, i.e., $\delta(M) = 0$. Now suppose $\dim M > 0$ and let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ denote the associated primes of M . Since $\dim M > 0$, \mathfrak{m} is not an associated prime, so that by prime avoidance, there is an element $x_1 \in \mathfrak{m} \setminus \bigcup_{i=1}^r \mathfrak{p}_i$. Let $M_1 = M/x_1 M$, so that $\dim M_1 \leq \dim M - 1$, and clearly $\delta(M) \leq \delta(M_1) + 1$, so that $\delta(M) \leq \dim M$, as desired. ■

THEOREM 3.14 (KRULL'S HAUPTIDEALSATZ). Let R be a Noetherian ring and $I = (a_1, \dots, a_r)$ a proper ideal in R . If \mathfrak{p} is a minimal prime ideal containing I , then $\text{ht } \mathfrak{p} \leq r$.

Proof. Note that $IR_{\mathfrak{p}}$ is an $\mathfrak{p}R_{\mathfrak{p}}$ -primary ideal, so that $\delta(R_{\mathfrak{p}}) \leq r$. Hence, $\text{ht } \mathfrak{p} = \dim R_{\mathfrak{p}} \leq r$. ■

THEOREM 3.15. Let \mathfrak{p} be a prime ideal of height $r \geq 0$ in a Noetherian ring R .

- (1) \mathfrak{p} is a minimal prime over some ideal (a_1, \dots, a_r) generated by r elements.
- (2) if $b_1, \dots, b_s \in \mathfrak{p}$, then $\text{ht } \mathfrak{p}/(b_1, \dots, b_s) \geq r - s$.
- (3) if a_1, \dots, a_r are as in (1), we have

$$\text{ht } \mathfrak{p}/(a_1, \dots, a_i) = r - i \quad \text{for } 1 \leq i \leq r.$$

Proof. (1) We have $\dim R_{\mathfrak{p}} = \text{ht } \mathfrak{p} = r$, so that there exist $\frac{a_1}{s_1}, \dots, \frac{a_r}{s_r} \in R_{\mathfrak{p}}$ generating an $\mathfrak{p}R_{\mathfrak{p}}$ -primary ideal. Let $I = (a_1, \dots, a_r)$. Then $IR_{\mathfrak{p}}$ is $\mathfrak{p}R_{\mathfrak{p}}$ -primary, so that \mathfrak{p} is a minimal prime over I , as desired.

- (2) Set $\bar{R} = A/(b_1, \dots, b_s)$ and $\bar{\mathfrak{p}} = \mathfrak{p}/(b_1, \dots, b_s)$. Let $t = \text{ht } \bar{\mathfrak{p}}$. Due to (1), there exist $\bar{c}_1, \dots, \bar{c}_t \in \bar{R}$ such that $\bar{\mathfrak{p}}$ is a minimal prime containing $(\bar{c}_1, \dots, \bar{c}_t)\bar{R}$. Pick lifts c_i of \bar{c}_i . Then \mathfrak{p} is a minimal prime containing $(b_1, \dots, b_s, c_1, \dots, c_t)$. By Theorem 3.14, $s + t \geq \text{ht } \mathfrak{p} = r$, as desired.
- (3) Note that $\bar{\mathfrak{p}} = \mathfrak{p}/(a_1, \dots, a_i)$ is a minimal prime containing $(\bar{a}_{i+1}, \dots, \bar{a}_r)$. Thus, due to Theorem 3.14, $\text{ht } \bar{\mathfrak{p}} \leq r - i$. But due to (2), $\text{ht } \bar{\mathfrak{p}} \geq r - i$ whence the equality follows. ■

§§ System of Parameters

II. HOMOLOGICAL METHODS

§4 Regular Sequences

§§ The Koszul Complex

DEFINITION 4.1. Let A be a ring and M an A -module. An element $a \in A$ is said to be *M-regular* if a is a non-zero-divisor on M . A sequence $\underline{a} = a_1, \dots, a_n$ is said to be an *M-sequence* if the following two conditions hold:

- (1) a_i is $M/(a_1, \dots, a_{i-1})M$ -regular for $1 \leq i \leq n$.
- (2) $M \neq (a_1, \dots, a_n)M$.

REMARK 4.2. Note that the permutation of an *M*-sequence need not be an *M*-sequence.

LEMMA 4.3. If a_1, \dots, a_n is an *M*-sequence, and if $a_1\xi_1 + \dots + a_n\xi_n = 0$ with $\xi_i \in M$ for $1 \leq i \leq n$, then $\xi_i \in (a_1, \dots, a_n)M$ for all $1 \leq i \leq n$.

Proof. Note that $a_n\xi_n = -a_1\xi_1 - \dots - a_{n-1}\xi_{n-1} \in (a_1, \dots, a_{n-1})M$, so that $\xi_n \in (a_1, \dots, a_{n-1})M$, and we can write

$$\xi_n = a_1\eta_1 + \dots + a_{n-1}\eta_{n-1}$$

for some $\eta_1, \dots, \eta_{n-1} \in M$. Substituting this back, we have

$$a_1(\xi_1 + a_n\eta_1) + \dots + a_{n-1}(\xi_{n-1} + a_n\eta_{n-1}) = 0.$$

Repeating our above argument, we have

$$\xi_{n-1} + a_n\eta_{n-1} \in (a_1, \dots, a_{n-2})M,$$

so that $\xi_{n-1} \in (a_1, \dots, a_n)M$. Continuing this way, we have our desired conclusion. ■

THEOREM 4.4. If a_1, \dots, a_n is an *M*-sequence, then so is $a_1^{m_1}, \dots, a_n^{m_n}$ for any positive integers m_1, \dots, m_n .

Proof. Note that it suffices to show that for any positive integer m , a_1^m, a_2, \dots, a_n is an M -sequence. We shall prove this statement by induction on $m \geq 1$. The base case with $m = 1$ is trivial. Since a_1 is M -regular, so is a_1^m . Suppose for $i > 1$, we have the relation

$$a_i \omega = a_1^m \xi_1 + \cdots + a_{i-1} \xi_{i-1} \quad \text{with} \quad \xi_j \in M.$$

Due to the induction hypothesis, we know that $a_1^{m-1}, a_2, \dots, a_i$ is an M -sequence, so that by Lemma 4.3, there exist $\eta_1, \dots, \eta_{i-1} \in M$ such that

$$\omega = a_1^{m-1} \eta_1 + a_2 \eta_2 + \cdots + a_{i-1} \eta_{i-1}.$$

Hence, we obtain

$$0 = a_1^{m-1} (a_1 \xi_1 - a_i \eta_1) + a_2 (\xi_2 - a_i \eta_2) + \cdots + a_{i-1} (\xi_{i-1} - a_i \eta_{i-1}).$$

Invoking Lemma 4.3 again,

$$a_1 \xi_1 - a_i \eta_1 \in (a_1^{m-1}, a_2, \dots, a_{i-1})M,$$

and hence,

$$a_i \eta_1 \in (a_1, \dots, a_{i-1})M.$$

But since a_1, \dots, a_i is an M -sequence,

$$\eta_1 \in (a_1, \dots, a_{i-1})M.$$

This shows that $\omega \in (a_1^m, a_2, \dots, a_{i-1})M$, as desired. ■

DEFINITION 4.5. Let A be a ring and $x_1, \dots, x_n \in A$. We define a complex K_\bullet as follows: set $K_0 = A$, and $K_p = 0$ if $p < 0$ or $p > n$. For $1 \leq p \leq n$, set

$$K_p = \bigoplus_{1 \leq i_1 < \cdots < i_p \leq n} Ae_{i_1, \dots, i_p}.$$

The differential $d: K_p \rightarrow K_{p-1}$ is defined by

$$d(e_{i_1, \dots, i_p}) = \sum_{k=1}^p (-1)^{k-1} x_{i_k} e_{i_1, \dots, \hat{i}_k, \dots, i_p} \in K_{p-1}$$

for $1 \leq p \leq n$, and $d = 0$ for $p \leq 0$ or $p > n$. This is called the *Koszul complex* corresponding to the sequence $\underline{x} = x_1, \dots, x_n$ and is often denoted by $K(\underline{x})$. If M is an A -module, we set $K(\underline{x}, M)_\bullet = K(\underline{x})_\bullet \otimes_A M$.

INTERLUDE 4.6 (TENSOR PRODUCT OF COMPLEXES). Let (A_\bullet, d) and (B_\bullet, d') be two complexes of R -modules. We define the complex $(A \otimes_R B)_\bullet$ as

$$(A \otimes_R B)_p = \bigoplus_{i+j=p} A_i \otimes_R B_j,$$

with the differential given by

$$d(a_i \otimes b_j) = da_i \otimes b_j + (-1)^i a_i \otimes db_j$$

where $a_i \in A_i$ and $b_j \in B_j$ for some integers i and j .

REMARK 4.7. It is straightforward to check that $K(\underline{x})_*$ is a complex, i.e., $d^2 = 0$. Further, for each $x \in A$, consider the complex $C(x)_*$ given by

$$\cdots \rightarrow 0 \rightarrow A \xrightarrow{\cdot x} A \rightarrow 0 \rightarrow \cdots$$

with A in degrees 0 and 1. One can then check that

$$K(\underline{x}) \cong C(x_1) \otimes_A \cdots \otimes_A C(x_n).$$

Since the tensor product of complexes is commutative (up to isomorphism), we note that permuting the sequence $\underline{x} = x_1, \dots, x_n$ results in an isomorphic complex.

DEFINITION 4.8. Let M be an A -module and $\underline{x} = x_1, \dots, x_n$ be a sequence in M . We define the *Koszul homology modules* to be the homology modules of the complex $K(\underline{x}, M)_*$ and are denoted $H_i(\underline{x}, M)$ for all $i \in \mathbb{Z}$.

It is straightforward to see that

$$H_0(\underline{x}, M) \cong M/(x_1, \dots, x_n)M \quad \text{and} \quad H_n(\underline{x}, M) = (0 :_M \underline{x}) = \{\xi \in M : x_1\xi = \cdots = x_n\xi = 0\}.$$

For a complex C_* and $x \in A$, let $C(x)_*$ denote the complex $C_* \otimes K(x)_*$.

THEOREM 4.9. Let C_* be a complex of A -modules and $x \in A$. Then there is an exact sequence of complexes

$$0 \rightarrow C_* \rightarrow C(x)_* \rightarrow \tilde{C}_* \rightarrow 0,$$

where \tilde{C}_* is given by $\tilde{C}_p = C_{p+1}$ with the same differential. This short exact sequence gives rise to a corresponding homology long exact sequence:

$$\cdots \rightarrow H_p(C_*) \rightarrow H_p(C(x)_*) \rightarrow H_{p-1}(C_*) = H_p(\tilde{C}_*) \xrightarrow{(-1)^{p-1}x} H_{p-1}(C_*) \rightarrow \cdots.$$

Further, we have $x \cdot H_p(C(x)_*) = 0$ for all $p \in \mathbb{Z}$.

Proof. Let d denote the differential of the complex C_* . The complex $K(x)_*$ is given by

$$\cdots \rightarrow 0 \rightarrow Ae_1 \xrightarrow{e_1 \mapsto x} A \rightarrow 0 \rightarrow \cdots,$$

so that we may identify

$$C(x)_p = C_p \oplus C_{p-1},$$

with the differential

$$\tilde{d}(\xi, \eta) = (d\xi + (-1)^{p-1}x\eta, d\eta).$$

Consider the short exact sequence of complexes:

$$\begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & C_p & \longrightarrow & C_{p-1} & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & C_p \oplus C_{p-1} & \longrightarrow & C_{p-1} \oplus C_{p-2} & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & C_{p-1} & \longrightarrow & C_{p-2} & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & \end{array}$$

where the vertical maps are the canonical inclusions and the projections. That these maps are indeed chain maps is easy to check.

It remains to compute the boundary map $H_p(\tilde{C}_\bullet) \rightarrow H_{p-1}(C_\bullet)$. Let $\eta \in \tilde{C}_p = C_{p-1}$ be such that $d\eta = 0$. Consider $(0, \eta) \in C_p \oplus C_{p-1}$ whose image under \tilde{d} is $((-1)^{p-1}x\eta, 0)$, which lifts to $(-1)^{p-1}x\eta \in C_{p-1}$. Thus, the boundary map $H_{p-1}(C_\bullet) \rightarrow H_{p-1}(C_\bullet)$ is multiplication by $(-1)^{p-1}x$.

Finally, we show that x annihilates $H_p(C(x)_\bullet)$. Indeed, let $(\xi, \eta) \in C_p \oplus C_{p-1}$ be such that $\tilde{d}(\xi, \eta) = 0$, equivalently, $d\xi = (-1)^p x\eta$ and $d\eta = 0$. Thus

$$x \cdot (\xi, \eta) = (x\xi, x\eta) = d(0, (-1)^p \xi),$$

consequently, x annihilates $H_p(C(x)_\bullet)$ for all $p \in \mathbb{Z}$. ■

COROLLARY 4.10. Let $\underline{x} = x_1, \dots, x_n$ be a sequence in A . Then (x_1, \dots, x_n) annihilates $H_p(\underline{x}, M)$ for all $p \in \mathbb{Z}$.

Proof. This follows from the fact that the Koszul complex is precisely $C(x_1) \otimes_A \cdots \otimes_A C(x_n) \otimes_A M$. ■

THEOREM 4.11. Let A be a ring, M an A -module, and $\underline{x} = x_1, \dots, x_n \in A$.

- (1) If \underline{x} is an M -sequence, then $H_p(\underline{x}, M) = 0$ for all $p \neq 0$ and $H_0(\underline{x}, M) = M/(x)\mathcal{M}$.
- (2) Suppose that (A, \mathfrak{m}) is a local ring, $x_1, \dots, x_n \in \mathfrak{m}$, and M is a finitely presented A -module. If $H_1(\underline{x}, M) = 0$ and $M \neq 0$, then \underline{x} is an M -sequence.

Proof. We prove both statements by induction on $n \geq 1$.

- (1) The base case with $n = 1$ is trivial, since $H_1(x_1, M) = (0 :_M x_1) = 0$ since x_1 is M -regular. Suppose now that $n > 1$. If $p > 1$, using Theorem 4.9 we have a long exact sequence:

$$0 = H_p(x_1, \dots, x_{n-1}, M) \rightarrow H_p(x_1, \dots, x_n, M) \rightarrow H_{p-1}(x_1, \dots, x_{n-1}, M) = 0$$

, where the two terms are zero from the inductive hypothesis. It follows that $H_p(x_1, \dots, x_n, M) = 0$ too. Next, if $p = 1$, then due to Theorem 4.9, we have an exact sequence

$$0 = H_1(x_1, \dots, x_{n-1}, M) \rightarrow H_1(x_1, \dots, x_n, M) \rightarrow H_0(x_1, \dots, x_{n-1}, M) = M/(x_1, \dots, x_{n-1})M \xrightarrow{x_n} M/(x_1, \dots, x_{n-1})M.$$

Since x_n is $M/(x_1, \dots, x_{n-1})M$ -regular, the last map in the above sequence is injective, so that $H_1(x_1, \dots, x_n, M) = 0$, as desired.

- (2) Again, the base case with $n = 1$ is trivial since $H_1(x_1, M) = (0 :_M x_1)$, which is zero if and only if x_1 is M -regular.

Since M is a finitely presented, all Koszul homology groups $K(x, M)$ of M must be finitely generated. The long exact sequence furnished by Theorem 4.9 is of the form

$$H_1(x_1, \dots, x_{n-1}, M) \xrightarrow{\cdot(-x_n)} H_1(x_1, \dots, x_{n-1}, M) \rightarrow H_1(x_1, \dots, x_n, M) = 0.$$

Thus the multiplication map by x_n on $H_1(x_1, \dots, x_{n-1}, M)$ is surjective. Since $x_n \in \mathfrak{m}$ and the Koszul homology is finitely generated, we must have that $H_1(x_1, \dots, x_{n-1}, M) = 0$ by Nakayama's lemma. Due to the inductive hypothesis, we must have that x_1, \dots, x_{n-1} is an M -sequence. Finally, due to Theorem 4.9, there is an exact sequence

$$0 = H_1(x_1, \dots, x_n, M) \rightarrow H_0(x_1, \dots, x_{n-1}, M) = M/(x_1, \dots, x_{n-1})M \xrightarrow{x_n} M/(x_1, \dots, x_{n-1})M,$$

so that the map $M/(x_1, \dots, x_{n-1})M \xrightarrow{x_n} M/(x_1, \dots, x_{n-1})M$ is injective, that is, x_n is $M/(x_1, \dots, x_{n-1})M$ -regular. ■

THEOREM 4.12. Let A be a Noetherian ring, M a finite A -module, and I an ideal in A with $IM \neq M$. For a positive integer $n > 0$, the following are equivalent:

- (1) $\text{Ext}_A^i(N, M) = 0$ for all $i < n$ and for any finite A -module N with $\text{Supp}_A(N) \subseteq V(I)$.
- (2) $\text{Ext}_A^i(A/I, M) = 0$ for all $i < n$.
- (3) $\text{Ext}_A^i(N, M) = 0$ for all $i < n$ and for some finite A -module N with $\text{Supp}_A(N) = V(I)$.
- (4) there exists an M -sequence of length n contained in I .

Proof. The implications (1) \Rightarrow (2) \Rightarrow (3) are clear.

(3) \Rightarrow (4) We shall prove this statement by induction on n . For the base case, suppose that $n = 1$, that is, $\text{Hom}_A(N, M) = 0$ where N is a finite A -module with $\text{Supp}_A(N) = V(I)$. If I does not contain a non-zero-divisor on M , then

$$I \subseteq \bigcup_{\mathfrak{p} \in \text{Ass}_A(M)} \mathfrak{p},$$

so that by Prime Avoidance, there exists an associated prime $\mathfrak{p} \in \text{Ass}_A(M)$ such that $I \subseteq \mathfrak{p}$ – in particular, $\mathfrak{p} \in V(I) = \text{Supp}_A(N)$, that is, $N_{\mathfrak{p}} \neq 0$. Due to Nakayama's lemma, this is equivalent to $N_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \kappa(\mathfrak{p}) \neq 0$. Thus, there is a non-zero $\kappa(\mathfrak{p})$ -linear, and hence $A_{\mathfrak{p}}$ -linear map $N_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \kappa(\mathfrak{p}) \rightarrow \kappa(\mathfrak{p})$. Further, since $\mathfrak{p} \in \text{Ass}_A(M)$, there is an injective A -linear map $A/\mathfrak{p} \hookrightarrow M$, which localizes into an injective $A_{\mathfrak{p}}$ -linear map $\kappa(\mathfrak{p}) \hookrightarrow M_{\mathfrak{p}}$. As a result, the composite:

$$N_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \kappa(\mathfrak{p}) \rightarrow \kappa(\mathfrak{p}) \hookrightarrow M_{\mathfrak{p}}$$

is non-zero. That is,

$$0 \neq \text{Hom}_{A_{\mathfrak{p}}}(N_{\mathfrak{p}}, M_{\mathfrak{p}}) = (\text{Hom}_A(N, M))_{\mathfrak{p}},$$

whence $\text{Ext}_A^0(N, M) = \text{Hom}_A(N, M) \neq 0$, a contradiction. Thus I must contain an M -regular element. This completes our proof of the base case.

Suppose now that $n > 1$. We know again that $\text{Ext}_A^i(N, M) = 0$ for $i < 1$, so by the above argument, I contains an M -regular element, say x_1 . Set $M_1 = M/x_1 M$. There is a short exact sequence

$$0 \rightarrow M \xrightarrow{x_1} M \rightarrow M_1 \rightarrow 0.$$

This gives rise to a long exact sequence:

$$\cdots \rightarrow \text{Ext}_A^i(N, M) \xrightarrow{x_1} \text{Ext}_A^i(N, M) \rightarrow \text{Ext}_A^i(N, M_1) \rightarrow \text{Ext}_A^{i+1}(N, M_1) \rightarrow \cdots.$$

If $i < n - 1$, then $\text{Ext}_A^i(N, M) = \text{Ext}_A^{i+1}(N, M) = 0$, so that $\text{Ext}_A^i(N, M) = 0$. Due to the inductive hypothesis, there exists an M_1 -sequence x_2, \dots, x_n contained in I . Hence, x_1, \dots, x_n is an M -sequence contained in I .

(4) \Rightarrow (1) We shall proceed by induction on $n \geq 1$. Consider the base case $n = 1$, that is, I contains an M -regular element x , and $\text{Supp}_A(N) \subseteq V(I)$. Since N is a finite A -module, $\text{Supp}_A(N) = V(\text{Ann}_A(N))$, so that $I \subseteq \sqrt{\text{Ann}_A(N)}$. Now x^r annihilates N for some $r > 0$ but x^r is still M -regular (Theorem 4.4). This immediately implies that $\text{Ext}_A^0(N, M) = \text{Hom}_A(N, M) = 0$, thereby establishing the base case.

Suppose now that $n > 1$, and let $x_1, \dots, x_n \in I$ be an M -sequence. Set $M_1 = M/x_1 M$ and consider the short exact sequence

$$0 \rightarrow M \xrightarrow{x_1} M \rightarrow M_1 \rightarrow 0,$$

which gives rise to the long exact sequence

$$\cdots \rightarrow \text{Ext}_A^{n-2}(N, M_1) \rightarrow \text{Ext}_A^{n-1}(N, M) \xrightarrow{x_1} \text{Ext}_A^{n-1}(N, M) \rightarrow \cdots.$$

Since I contains an M_1 -sequence of length $n - 1$, due to the inductive hypothesis, $\text{Ext}_A^{n-2}(N, M) = 0$, that is, multiplication by x_1 induces an injective map on $\text{Ext}_A^{n-1}(N, M)$. Now, as we have observed above, $I \subseteq \sqrt{\text{Ann}_A(N)}$, so that there is a positive integer $r > 0$ such that x_1^r annihilates N , and hence must annihilate $\text{Ext}_A^{n-1}(N, M)$. This is possible if and only if $\text{Ext}_A^{n-1}(N, M) = 0$, as desired. ■